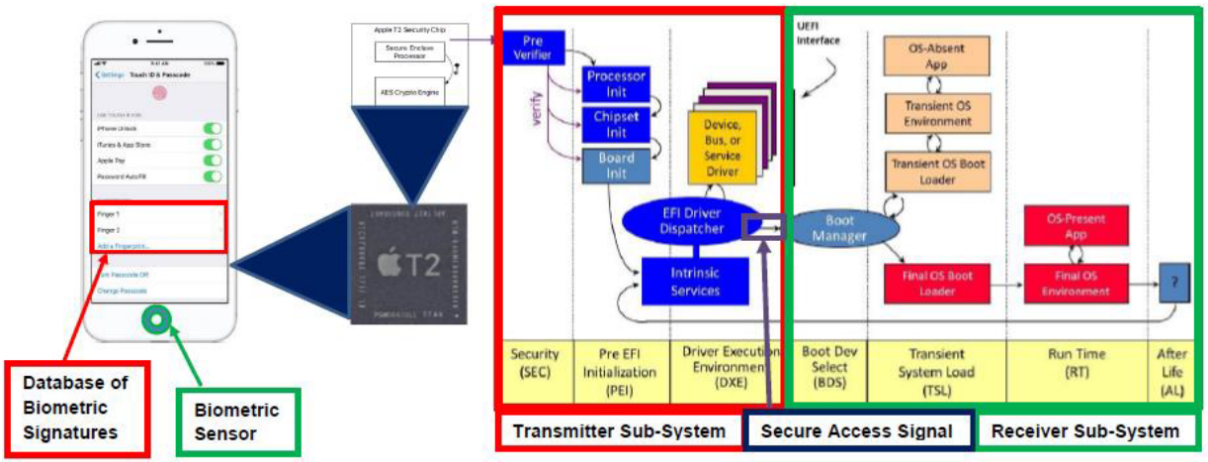
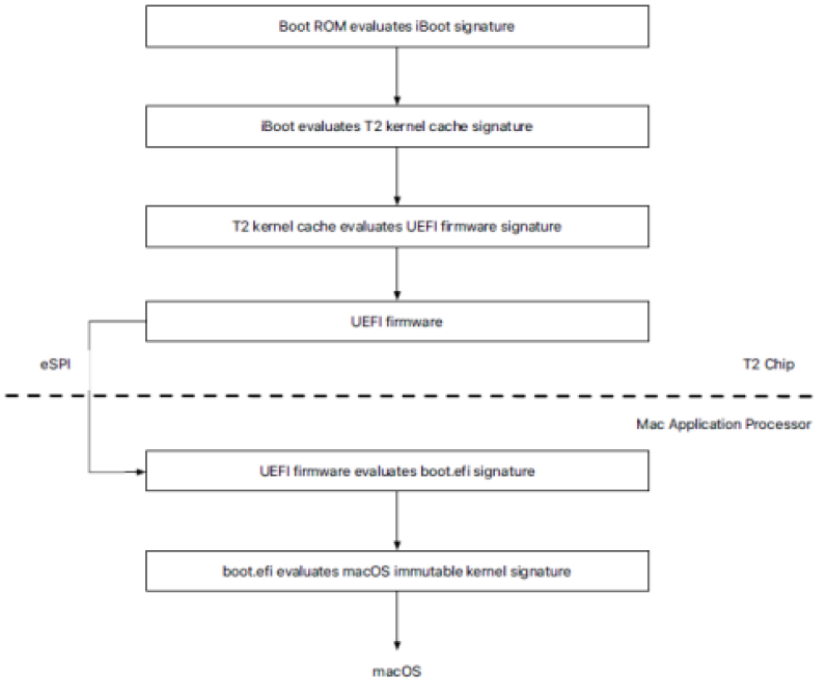
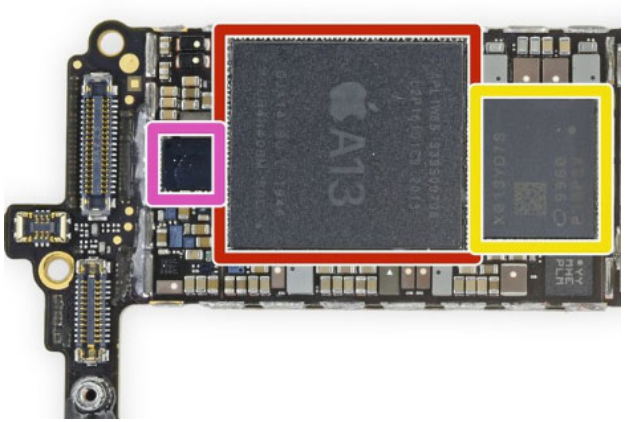
EXHIBIT G

Claim Chart for U.S. Patent No. 9,269,208 ("the '208 Patent")

The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone type cellular phones and Apple iPad type tablets, including the Apple iPhone SE (2nd generation) and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '208 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '208 Patent literally and, to the extent not literally, under the doctrine of equivalents.

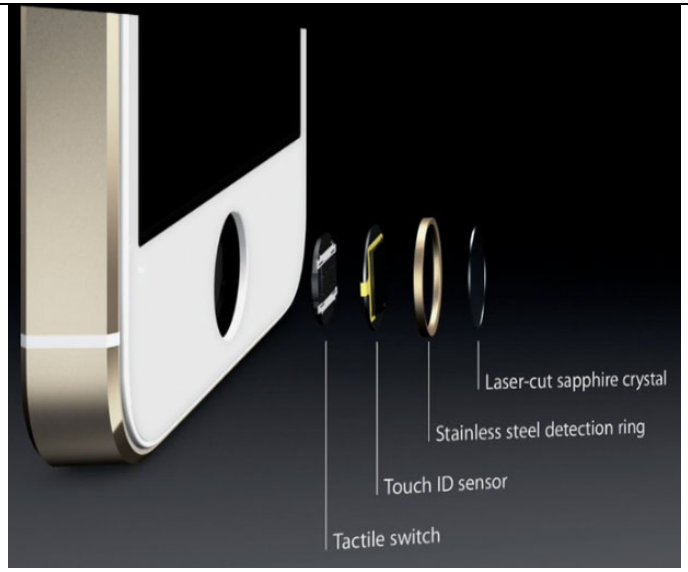
Claim 10	Apple iPhone SE (2nd generation)
10. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled item dependent upon information in said secure	To the extent that the preamble is deemed to be a limitation, the Apple iPhone SE is configured to use a system in accordance with this claim. Apple's Touch ID secure access technology, as implemented in, e.g., Apple's iPhone, is described in various Apple publications, such as Apple T2 Security Chip Security Overview (Oct. 2018) and iOS Security (Sept. 2014). Further, the Apple T2 security Chip implementing such access technology is the subject of third party analyses, such as Davidov, M., et al., Inside the Apple T2. Finally, the subject technology is described in Apple patent documents, such as U.S. Patent Appl. No. 2014/0089682. Such information evidences the operation of Apple's Touch ID technology in the manner depicted below: 

Claim 10	Apple iPhone SE (2nd generation)
access signal, the method comprising the steps of:	As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green). In the figure below, the transmission is from the T2 Chip to the Mac Application Processor via the Enhanced Serial Peripheral Interface ("eSPI") bus:  *Apple T2 Security Chip Security Overview* (Oct. 2018) at 8.
10a. populating the database of biometric signatures by: receiving a	**The Apple iPhone SE populates the database of biometric signatures by receiving a series of entries of the biometric signal.**

Claim 10	**Apple iPhone SE (2nd generation)**
series of entries of the biometric signal;	More specifically, the Apple iPhone SE has a secure enclave in the A13 chip that populates a database of a mathematical representation of fingerprints used for Touch ID. The Apple iPhone SE receives a series of fingerprints signal through a sensor located on a home button. **Secure Enclave** The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data. Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587 

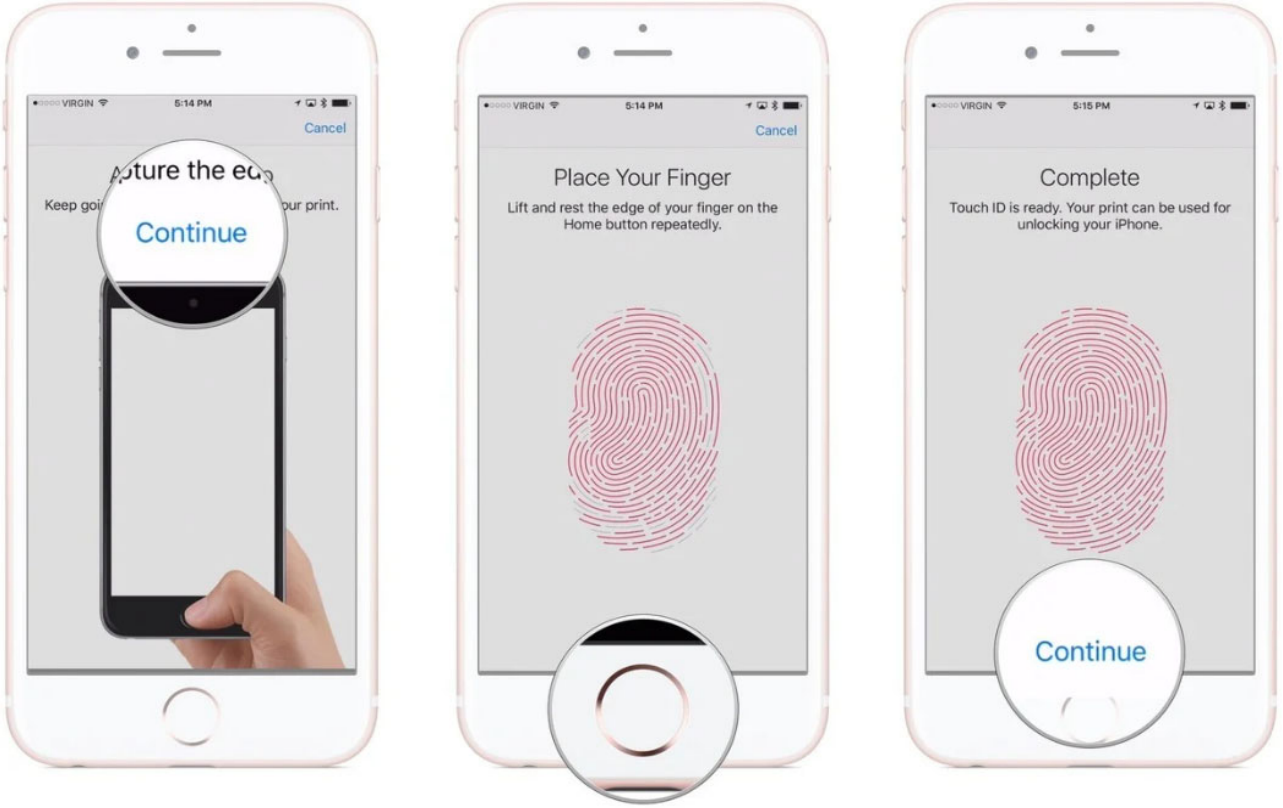
Claim 10	Apple iPhone SE (2nd generation)
	• Apple APL1W85 A13 Bionic SoC layered over Samsung K3UH4H40BM-SGCL (presumably 3 GB LPDDR4X) https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066 The Apple iPhone SE has a home button that includes a sensor to detect fingerprints and activates a Touch ID to start reading the user's fingerprint. **Advanced technologies** The technology within Touch ID is some of the most advanced hardware and software that we've put into any device. The button is made from sapphire crystal—one of the clearest, hardest materials available. This protects the sensor and acts as a lens to precisely focus it on your finger. On iPhone and iPad, a steel ring surrounding the button detects your finger and tells Touch ID to start reading your fingerprint. The sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy. https://support.apple.com/en-us/HT204587

Claim 10	**Apple iPhone SE (2nd generation)**
	 https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

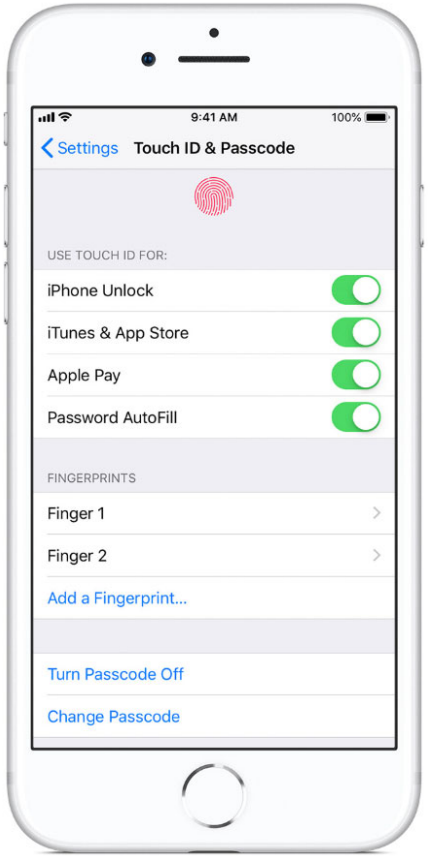
Claim 10	**Apple iPhone SE (2nd generation)**
	 https://www.imore.com/how-touch-id-works

Claim 10	Apple iPhone SE (2nd generation)
	Set up Touch ID Before you can set up Touch ID, you need to create a passcode for your device.* Then follow these steps: 1. Make sure that the Home button and your finger are clean and dry. 2. Tap Settings > Touch ID & Passcode, then enter your passcode. 3. Tap Add a Fingerprint and hold your device as you normally would when touching the Home button. 4. Touch the Home button with your finger—but don't press. Hold it there until you feel a quick vibration, or until you're asked to lift your finger. 5. Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time. 6. The next screen asks you to adjust your grip. Hold your device as you normally would when unlocking it, and touch the Home button with the outer areas of your fingertip, instead of the center portion that you scanned first. https://support.apple.com/en-us/HT201371

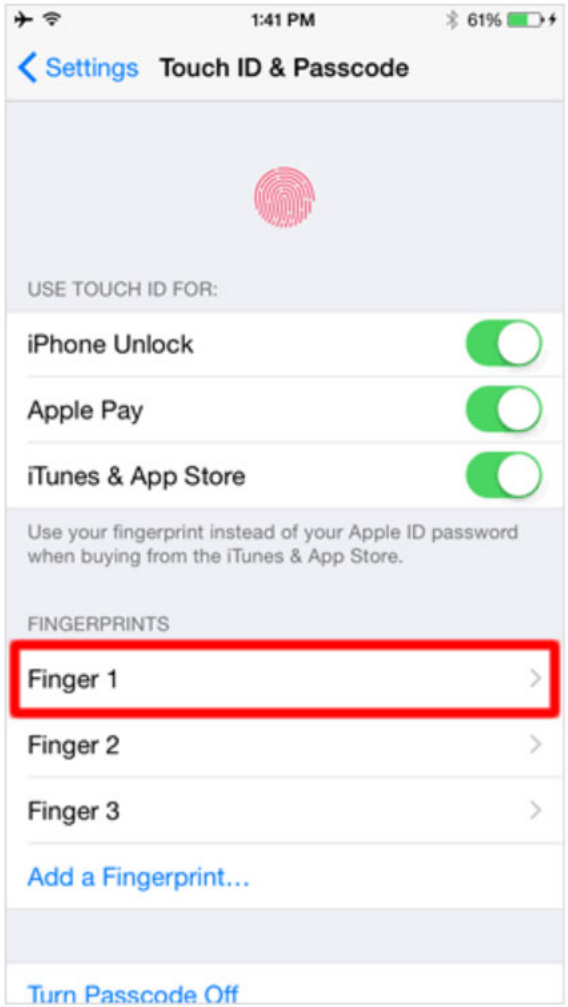
Claim 10	Apple iPhone SE (2nd generation)

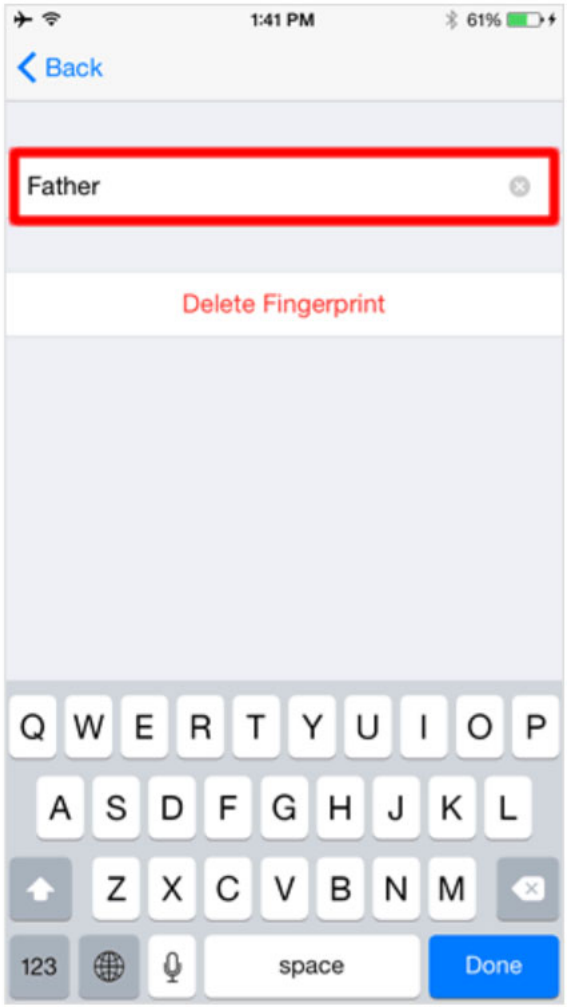


https://www.imore.com/how-to-use-touch-id-iphone-ipad

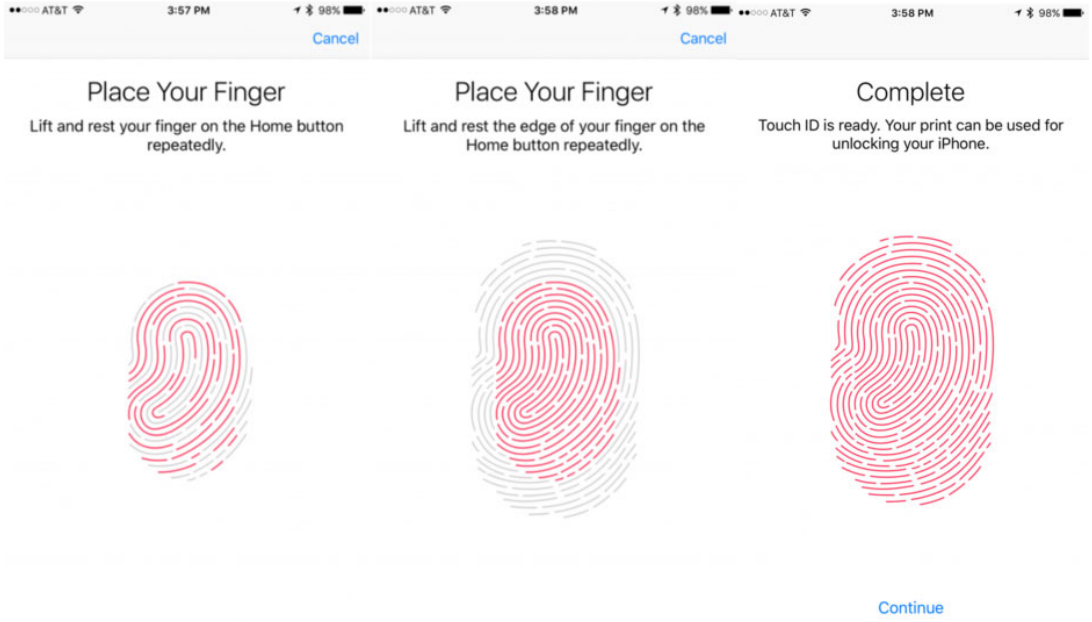
Claim 10	**Apple iPhone SE (2nd generation)**
	Additionally, the Apple iPhone SE allows users to add multiple fingerprints and label each fingerprint whatever they prefer. It makes it easier to recognize different fingerprints when users share their device with other family members or friends.   https://www.howtogeek.com/205525/how-to-add-touch-id-fingerprints-to-iphone-or-ipad/

Claim 10	Apple iPhone SE (2nd generation)

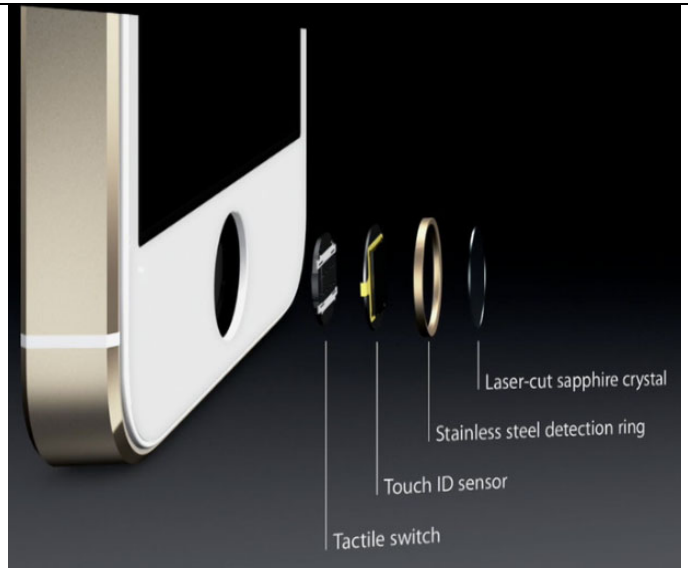




https://en.teach-me.biz/iphone/settings/touch-id.html

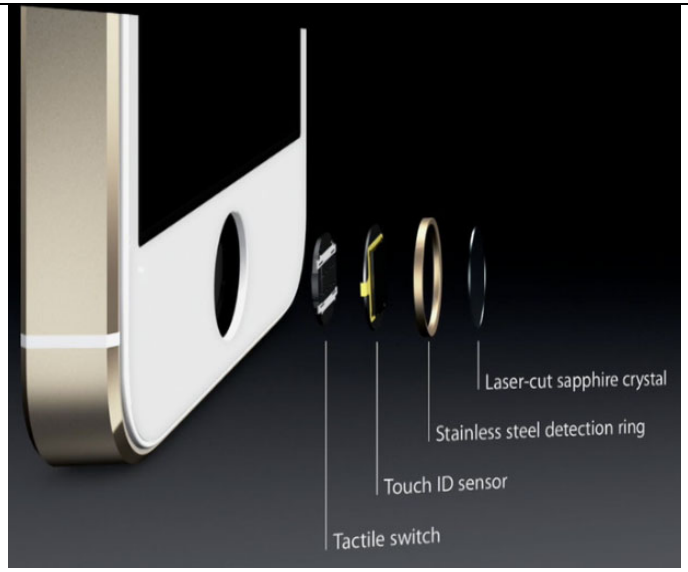
Claim 10	**Apple iPhone SE (2nd generation)**
10a1. determining at least one of the number of said entries and a duration of each said entry;	**The Apple iPhone SE populates the database of biometric signatures by determining at least one of the number of said entries and a duration of each said entry.** More specifically, the Apple iPhone SE receives a series of fingerprint signal through a sensor by having users to touch a home button repeatedly to set up a Touch ID.  https://www.idownloadblog.com/2016/01/14/touch-id-not-working-try-this/

Claim 10	**Apple iPhone SE (2nd generation)**
	 https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

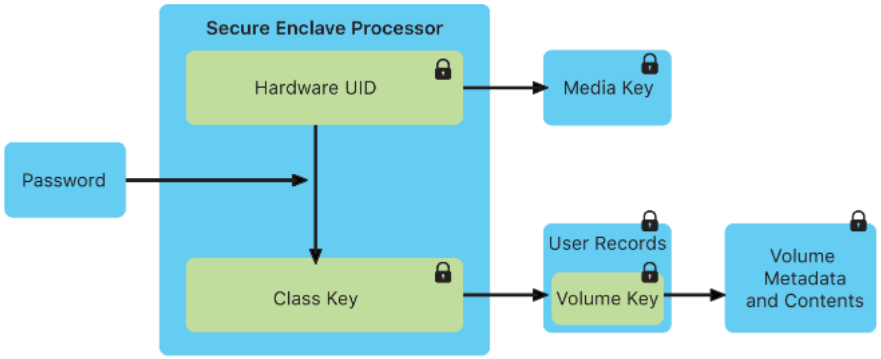
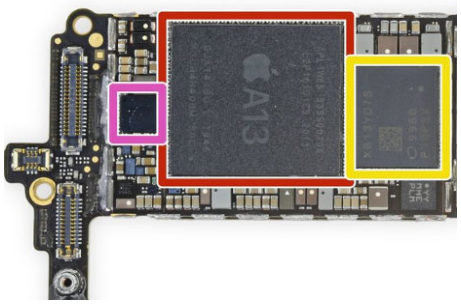
Claim 10	**Apple iPhone SE (2nd generation)**
	 https://www.imore.com/how-touch-id-works
10a2. mapping said series into an instruction; and	**The Apple iPhone SE populates the database of biometric signatures by mapping said series into an instruction.** More specifically, the Apple iPhone SE includes a secure enclave processor (SEP) that can map a series of fingerprint signal into an instruction for encryption. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.

Claim 10	Apple iPhone SE (2nd generation)
	Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587
10a3. populating the database according to the instruction;	**The Apple iPhone SE populates the database of biometric signatures according to the instruction.** More specifically, the Apple iPhone SE includes a secure enclave processor (SEP) that can generate the encrypted fingerprint data based on the instruction to determine whether the device can be unlocked. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy. Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587

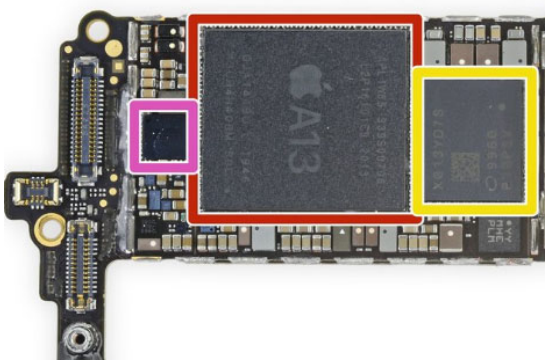
Claim 10	Apple iPhone SE (2nd generation)
10b. receiving a biometric signal;	**The Apple iPhone SE provide secure access to a device by receiving a fingerprint signal.** More specifically, the Apple iPhone SE receives a fingerprint signal through a sensor and determines whether to unlock the device.  https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

Claim 10	**Apple iPhone SE (2nd generation)**
	 https://www.imore.com/how-touch-id-works
10c. matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;	**The Apple iPhone SE provide secure access to a device by matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.** More specifically, the Apple iPhone SE has a secure enclave processor (SEP) that matches fingerprints against the registered fingerprint data. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.

Claim 10	Apple iPhone SE (2nd generation)
	Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587 Further, U.S. Patent No. 2016/0125223, an abandoned patent assigned to Apple which upon information and belief describes the accused Apple's Touch ID, provides that there is a transmitter sub-system that provides a matching score of sensed fingerprint against the fingerprint data stored in the memory.
10d. emitting a secure access signal conveying information dependent upon said accessibility attribute; and	**The Apple iPhone SE provide secure access to a device by emitting a secure access signal conveying information dependent upon said accessibility attribute** More specifically, the iPhone SE includes a secure enclave processor (SEP) that includes a transmitter block and sends a secure access signal based on the fingerprints data received from the sensor. When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but can't read it. It's encrypted and authenticated with a session key that is negotiated using a shared key provisioned for each Touch ID sensor and its corresponding Secure Enclave at the factory. The shared key is strong, random, and different for every Touch ID sensor. The session key exchange uses AES key wrapping, with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption. https://support.apple.com/guide/security/touch-id-security-sec0f02a0f7f/web

Claim 10	Apple iPhone SE (2nd generation)
	The Secure Enclave also maintains the integrity of its cryptographic operations even if the device kernel has been compromised. Communication between the Secure Enclave and the application processor is tightly controlled by isolating it to an interrupt-driven mailbox and shared memory data buffers.  The Secure Enclave processor. https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web  • Apple APL1W85 A13 Bionic SoC layered over Samsung K3UH4H40BM-SGCL (presumably 3 GB LPDDR4X) https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

Claim 10	**Apple iPhone SE (2nd generation)**
10e. providing conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	**The Apple iPhone SE provides conditional access to the controlled item dependent upon said information, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.** More specifically, the iPhone SE includes an application processor (AP) that can grant access to the device based on the matching fingerprints data received from a secure enclave processor (SEP). Secure Enclave The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data. Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587

Claim 10	**Apple iPhone SE (2nd generation)**
	 • Apple APL1W85 A13 Bionic SoC layered over Samsung K3UH4H40BM-SGCL (presumably 3 GB LPDDR4X) https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066